

CLAIMS:

1. A method of identifying and/or verifying hardware and/or software of an appliance (23) and of a data carrier (9) which is provided to cooperate with the appliance, comprising the following steps:

- transmitting first authorization data of the hardware and/or software to a first
5 unit (E1),
- comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit (E1) with first verification data stored in the first unit (E1),
- authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or
10 software and the first verification data stored in the first unit (E1),
- transmitting second authorization data of a data carrier (9) to a second unit (E2),
- comparing the second authorization data in the second unit (E2) with second verification data stored in the second unit (E2),
- 15 - authorizing the data carrier (9) if there is coincidence between the second authorization data and the second verification data stored in the second unit (E2),
- wherein a direct data exchange is carried out between the first unit (E1) and the second unit (E2).

20 2. A method as claimed in claim 1, wherein the direct data exchange between the first unit (E1) and the second unit (E2) comprises a transmission of encrypted data and a comparison and/or decryption of data transmitted between the first unit (E1) and the second unit (E2).

25 3. A method as claimed in claim 1 or 2, wherein the data exchange between the first unit (E1) and the second unit (E2) is carried out prior to an identification and/or verification of first authorization data of the hardware and/or software and of second authorization data of the data carrier (9).

4. A method as claimed in any of claims 1, 2 or 3, wherein a central arithmetic unit (2) of the first unit (E1) and a central arithmetic unit (10) of the second unit (E2) jointly access at least one ROM memory (18), one RAM memory (19) and/or one non-volatile memory (20).

5

5. A method as claimed in any of claims 1 to 4, wherein encryption (6, 14) of the first authorization data and of the second authorization data is carried out in the first unit (E1) and in the second unit (E2).

10

6. A method as claimed in any of claims 1 to 5, wherein the second authorization data are obtained from a smartcard or a tag or a label that forms the data carrier (9).

7. A circuit for identifying and/or verifying hardware and/or software of an appliance (23) and of a data carrier (9) which is provided to cooperate with the appliance, comprising:

15

- a first unit (E1) for identifying and/or verifying the hardware and/or software of the appliance, comprising a central arithmetic unit (2) and at least one memory (3, 4, 5, 18, 19, 20) and an interface (7, 22) to the hardware and/or software that is to be identified and/or verified, and

20

- a second unit (E2), comprising a central arithmetic unit (10) and at least one memory (11, 12, 13, 18, 19, 20) and an interface (16) to an external data carrier (9) and also an interface (15) to the hardware and/or software,

- wherein a communication interface (17) is provided between the central arithmetic units (2, 10) of the first unit (E1) and the second unit (E2).

25

8. A circuit as claimed in claim 7, wherein the memories of the first unit (E1) and of the second unit (E2) are formed by a ROM memory (3, 11, 18) and a RAM memory (4, 12, 19) and/or a non-volatile memory (5, 13, 20).

30

9. A circuit as claimed in claim 7 or 8, wherein the ROM memories and/or the RAM memories and/or the non-volatile memories of the first unit (E1) and of the second unit (E2) are in each case combined to form a common ROM memory (18) and/or a common RAM memory (19) and/or a common non-volatile memory (20).

10. A circuit as claimed in any of claims 7 to 9, wherein the first unit (E1) and the second unit (E2) in each case comprise an encryption device (6, 14).

11. A circuit as claimed in any of claims 7 to 10, wherein the central arithmetic unit of the first unit (E1) and the central arithmetic unit of the second unit (E2) are combined to form a common central arithmetic unit (21), which common central arithmetic unit (21) has the integrated communication interface, and wherein the common central arithmetic unit (21) is connected by an interface (22) to the hardware and/or software that is to be identified and/or verified.

12. A circuit as claimed in any of claims 7 to 11, wherein the interface (16) to the external data carrier (9) is designed for contactless communication with the external data carrier (9).

13. A circuit as claimed in any of claims 7 to 12, wherein the external data carrier (9) is formed by a smartcard or a tag or a label.

14. An appliance which comprises as hardware at least one central arithmetic unit (8), which central arithmetic unit (8) is designed to run software and to obtain data from an external data carrier (9) cooperating with the appliance, wherein a circuit (1) as claimed in any of claims 7 to 13 is coupled to the central arithmetic unit (8).

15. An appliance as claimed in claim 14, wherein the central arithmetic unit (8) of the appliance (23) is coupled via an interface integrated in the central arithmetic unit (8) of the appliance to the circuit (1, SM) integrated in the central arithmetic unit (8).